Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
	)	
	)	
Wireless E911 Location Accuracy Requirements	)	PS Docket No. 07-114
	)	

To: The Commission

COMMENTS OF PUBLIC KNOWLEDGE

Public Knowledge (PK) files these comments in the Commission's *Fourth Further Notice of Proposed Rulemaking* (FNPRM) to highlight specific privacy concerns in the handling of extremely sensitive geolocation information. Although PK agrees with the Commission that protecting life and safety requires that mobile devices capable of calling 911 must provide precise location information, including building floor number and other height related information generally referred to as "Z-Axis" information, PK must express grave concern over the handling of this information by carriers. In particular, recent comments by AT&T in response to Commissioner Rosenworcel's inquiry on reports of recent data breaches and sales of geolocation information – and specifically A-GPS information – make clear that the Commission must clarify that all information collected pursuant to the Commission's E911 enhanced geolocation mandate is subject not merely to standard CPNI protections, but to the enhanced secure storage requirements associated with the NEAD database.

ARGUMENT

As the Commission has recognized since the third *Further Notice of Proposed Rulemaking* in this proceeding, a government mandate for enhanced geolocation information, including dispatchable address information for 911 response, raises significant concerns around

consumer privacy.[1] In the Third Report and Order adopted in 2015, the Commission reaffirmed that information collected either for inclusion in the NEAD or "***any other information*** involved in the determination and delivery of dispatchable location" required additional safeguards above and beyond those usually associated with the Commission's CPNI regulations.[2] Specifically, the Commission required:

> that, as a condition of using the NEAD or any information contained therein to meet our 911 location requirements, ***and prior to use of the NEAD***, CMRS providers must certify that they will not use the NEAD ***or associated data*** for any purpose other than for the purpose of responding to 911 calls, except as required by law. ***Additionally,*** should aspects of a CMRS provider's dispatchable location operations ***not be covered by the NEAD privacy and security plan***, the provider should file an addendum ***to ensure that the protections outlined in the NEAD plan will cover the provider's dispatchable location transactions end-to-end***.

Id. (emphasis added)

In short, as the Commission stated in the clearest and most unambiguous terms, all information associated with dispatchable location information, whether stored in the NEAD or not, must receive the highest degree of protection. This includes maintaining an appropriate standard of security to prevent unintended/accidental disclosures over and above the requirements already imposed by the Commission to protect CPNI.[3] The Commission should re-affirm that the protections applicable to the NEAD database to Z-axis information regardless of whether or not it is technically stored in the NEAD database. This should include the requirement that carriers file an addendum to their existing NEAD security plans, and require

---

[1] *See* Wireless E911 Location Accuracy Requirements, *Third Further Notice of Proposed Rulemaking*, 29 FCC Rcd 2374 ¶136 (2014) (*Third Further Notice*).
[2] Wireless E911 Location Accuracy Requirements, *Third Report and Order*, 30 FCC Rcd 1259 ¶71 (2015) (*Third R&O*) (emphasis added).
[3] *See, e.g.,* Implementation of Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, 22 FCC Rcd 6927 ¶¶64-65 (2007) (*2007 Pretexting Order*).

additional certification by carriers that they will not use the Z-Axis information, or any associated information, for any purpose other than E911 or as required by law. Indeed, were it not for recent activities by carriers, and the recent letters by AT&T, Sprint, and T-Mobile to Commissioner Jessica Rosenworcel[4] implying that A-GPS data is somehow not covered by the sweeping protections adopted in the *Third R&O*, the inclusion of Z-Axis information in the requirements set forth in the *Third R&O* would be obvious.

The 3 named carriers all appear to imply that the information associated with dispatchable address information, including specifically A-GPS information, is not included in the heightened protections set forth in *Third R&O* at ¶¶69-73. Instead, they focus on the fact that (a) the NEAD database remains in development; and (b) the NEAD database contains a set of addresses associated with the MAC addresses of Wi-Fi- devices and Bluetooth beacons for purposes of providing dispatchable address information. As the plain language of the *Third R&O* makes plain, however, these distinctions are irrelevant. The *Third R&O* explicitly recognized that work on dispatchable address information, as well as x-axis, y-axis and z-axis coordinates, would begin before the NEAD was ready.[5] This is why the *Third R&O* used such clear and unambiguous language with regard to the responsibility to protect information which would reveal the precise address of a device. Indeed, to the extent carriers believed that A-GPS or other information was not covered by the NEAD database protections, the *Third R&O* required them

---

[4] *See Letter of Joan Marsh, Chief Regulatory & State External Affairs Officer, to Commissioner Jessica Rosenworcel* (May 15, 2019); *Letter of Maureen Cooney, Head of Privacy, Sprint to Commissioner Jessica Rosenworcel* (May 15, 2019); *Letter of Kathleen O'Brien Ham, Senior Vice President, Government Affairs, T-Mobile USA to Commissioner Jessica Rosenworcel* (May 15, 2019). Available at: https://docs.fcc.gov/public/attachments/DOC-357494A2.pdf

[5] *Third R&O* at ¶69 n.167.

to file "an addendum to ensure that the protections outlined in the NEAD plan will cover the provider's dispatchable location transactions end-to-end."[6]

Given the public statements of carriers implying that the additional protections applicable to the NEAD apply to all of a "provider's dispatchable location transactions end-to-end," the Commission should not merely reassert this responsibility with regard to any additional location data the Commission may require in this proceeding. The Commission should also remind carriers in the strongest terms of their existing responsibilities, and conduct a thorough investigation to ensure that carriers are in compliance. As part of the carriers' "dispatchable location transactions," carriers receive highly sensitive data protected by law. Cable operators, for example, may not turn over their address-linked information unless carriers demonstrate that it will not be used for any purposes other than 911, unless otherwise required by law.[7] Without adequate safeguards to protect "dispatchable location transactions end-to-end," cable operators face a choice between risking liability or withholding subscriber address information. This would clearly frustrate the goal of providing the most detailed information possible to first responders, while protecting the information from any other use or exposure.

[6] *Id.* at ¶71.
[7] 47 U.S.C. §551.

CONCLUSION

For the reasons stated above, the Commission should reaffirm the applicability of the enhanced privacy protection and security requirements established in the *Third R&O* to any new information required in this proceeding.

Respectfully submitted,

X_____

Harold Feld
Senior Vice President
Public Knowledge
1818 N. St., NW
Suite 410
Washington, DC 20036
(202) 681-0020